IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
NORFOLK DIVISION

VIR2US, INC.	)	
	)	
Plaintiff and Counterclaim Defendant,	)	C.A. No. 2:15-cv-162-HCM-LRL
	)	
v.	)	
	)	
INVINCEA, INC., and	)	
INVINCEA LABS, LLC	)	
	)	
Defendants and Counterclaim Plaintiffs.	)	

DECLARATION OF DR. AVIEL D. RUBIN IN SUPPORT
OF INVINCEA'S OPENING BRIEF ON CLAIM CONSTRUCTION

I. INTRODUCTION

1. I, Aviel D. Rubin, Ph. D., have been retained by Cooley LLP, which represents Defendants-Counterclaim Plaintiffs Invincea, Inc. and Invincea Labs, LLC ("Invincea") in connection with its litigation against Plaintiff-Counterclaim Defendant Vir2us, Inc. ("Vir2us). I submit this declaration to explain what a person of ordinary skill in the art would understand certain terms of the claims of the patents in suit to mean, when viewed in the context of the intrinsic evidence and the general knowledge of a person of ordinary skill. If called to testify on these matters, I would testify substantially as set forth herein.

II. BACKGROUND AND QUALIFICATIONS

A. Education

2. I possess the knowledge, skills, experience, training and the education to form an expert opinion and testimony in this matter. I have 22 years of experience in the field of computer science, and specifically in Internet and computer security. I received my Ph.D. in Computer Science and Engineering from the University of Michigan, Ann Arbor in 1994, with a specialty in computer security and cryptographic protocols. My thesis was entitled "Nonmonotonic Cryptographic Protocols" and concerned authentication in long-running networking operations.

B. Career

3. I will discuss my current position as a professor first, followed by a synopsis of my career and work from when I received my Ph.D. to the present.

4. I am currently employed as Professor of Computer Science at Johns Hopkins University, where I perform research, teach graduate courses in computer science and related subjects, and supervise the research of Ph.D. candidates and other students. Courses I have taught include Security and Privacy in Computing and Advanced Topics in Computer Security. I am also the Technical Director of the Johns Hopkins University Information Security Institute, the University's focal point for research and education in information security, assurance, and privacy. The University, through the Information Security Institute's leadership, has been

designated as a Center of Academic Excellence in Information Assurance by the National Security Agency and leading experts in the field. The focus of my work over my career has been computer security, and my current research concentrates on systems and networking security, with special attention to software and network security.

5. After receiving my Ph.D., I began working at Bellcore in its Cryptography and Network Security Research Group from 1994 to 1996. During this period I focused my work on Internet and Computer Security. While at Bellcore, I published an article titled "Blocking Java Applets at the Firewall" (Martin, Ex. 1047) about the security challenges of dealing with JAVA applets and firewalls, and a system that we built to overcome those challenges.

6. In 1997, I moved to AT&T Labs, Secure Systems Research Department, where I continued to focus on Internet and computer security. From 1995 through 1999, in addition to my work in industry, I served as Adjunct Professor at New York University, where I taught undergraduate classes on computer, network and Internet security issues.

7. I stayed in my position at AT&T until 2003, when I left to accept a full time academic position at Johns Hopkins University. The University promoted me to full professor with tenure in April, 2004.

8. I serve, or have served, on a number of technical and editorial advisory boards. For example, I served on the Editorial and Advisory Board for the International Journal of Information and Computer Security. I also served on the Editorial Board for the Journal of Privacy Technology. I have been Associate Editor of IEEE Security and Privacy Magazine, and served as Associate Editor of ACM Transactions on Internet Technology. I am currently an Associate Editor of the journal Communications of the ACM. I was an Advisory Board Member of Springer's Information Security and Cryptography Book Series. I have served in the past as a member of the DARPA Information Science and Technology Study Group, a member of the Government Infosec Science and Technology Study Group of Malicious Code, a member of the AT&T Intellectual Property Review Team, Associate Editor of Electronic Commerce Research Journal, Co-editor of the Electronic Newsletter of the IEEE Technical Committee on Security

and Privacy, a member of the board of directors of the USENIX Association, the leading academic computing systems society, and a member of the editorial board of the Bellcore Security Update Newsletter.

9. I have spoken on information security and electronic privacy issues at more than 50 seminars and symposia. For example, I presented keynote addresses on the topics "Security of Electronic Voting" at Computer Security 2004 Mexico in Mexico City in May 2004; "Electronic Voting" to the Secure Trusted Systems Consortium 5th Annual Symposium in Washington DC in December 2003; "Security Problems on the Web" to the AT&T EUA Customer conference in March, 2000; and "Security on the Internet" to the AT&T Security Workshop in June 1997. I also presented a talk about hacking devices at the TEDx conference in October 2011 and also another TEDx talk on the same topic in September 2015.

10. I was founder and President of Independent Security Evaluators (ISE), a computer security consulting firm, from 2005-2011. In that capacity, I guided ISE through the qualification as an independent testing lab for Consumer Union, which produces Consumer Reports magazine. As an independent testing lab for Consumer Union, I managed an annual project where we tested all of the popular anti-virus products. Our results were published in Consumer Reports each year for three consecutive years. I am currently the founder and managing partner of Harbor Labs, a software and networking consulting firm.

11. As is apparent from the above description, virtually my entire professional career has been dedicated to issues relating to information and network security. Moreover, through my consulting work and my work at AT&T and Bellcore, I am familiar with the practical aspects of designing, analyzing, and deploying security applications in network environments.

C. Publications

12. I am a named inventor on ten United States patents, all in the information security area. The patent numbers and titles as well as my co-inventors are listed on the attached curriculum vitae. (*See* App'x A.)

13. In March 2004, I was asked by the Federal Trade Commission to submit a report commenting on the viability and usefulness of a national do not e-mail registry. I submitted my report entitled "A Report to the Federal Trade Commission on Responses to Their Request for Information on Establishing a National Do Not E-mail Registry" on May 10, 2004.

14. I have also testified before Congress regarding the security issues with electronic voting machines and in the United States Senate on the issue of censorship. I also testified in Congress on November 19, 2013 about security issues related to the government's Healthcare.gov web site.

15. I am author or co-author of five books regarding information security issues: *Brave New Ballot*, Random House, 2006; *Firewalls and Internet Security* (second edition), Addison Wesley, 2003; *White-Hat Security Arsenal*, Addison Wesley, 2001; *Peer-to-Peer*, O'Reilly, 2001; and *Web Security Sourcebook*, John Wiley & Sons, 1997. I am also the author of numerous journal and conference publications.

D. Curriculum Vitae

16. Additional details of my education and employment history, recent professional service, patents, publications, and other testimony are set forth in my current curriculum vitae, attached to this declaration as App'x A.

III. LEGAL UNDERSTANDING

17. I have been informed by counsel and understand that the disclosure of the patents is to be viewed from the perspective of one of ordinary skill in the art at the time of the patent's effective filing date. I have also been informed by counsel and understand that the words of a patent claim are generally given their ordinary and customary meaning to one of ordinary skill in the art at the time the patent was filed. However, counsel informs me that where a patentee has used the specification to define terms of the patent in a manner that differs from the plain and ordinary meaning of those terms, the terms should be used as defined by the patentee to the extent that the definition is consistent with the specification. I further understand from counsel that the claims,

specification, and the prosecution history of a patent must be considered in interpreting the language in the patent claims. At the same time, I have been informed by counsel and understand that the specification cannot be used to read limitations into the claim.

18. To construe the claim terms, I therefore reviewed the patent claims, specification, and prosecution history of the U.S. Patent Nos. 7,392,541 ("'541 patent"), 7,536,598 ("'598 patent"), and 8,839,422 ("'422 patent"). The conclusions herein are based on the understanding of one of ordinary skill in the art at the time the '541, the '598, and the '422 patents were filed.

19. I have been informed by counsel and understand that, in some circumstances, a patentee may claim a particular structure by reciting the function performed by that structure in the patent claim. I understand that this method of claiming is typically indicated by the use of the words "means" or "means for" in the claim language. I further understand that these types of claim limitations are typically referred to as "means-plus-function" claim limitations.

20. I have been informed by counsel and understand that the absence of the word "means" does not necessarily preclude the interpretation of that claim term as a means-plus-function element. I have been informed and understand that the key consideration is whether the claim term connotes sufficient structure to one of ordinary skill in the art to perform the claimed function. I understand that if the claim term connotes sufficient structure to inform one of ordinary skill in the art for performing the claimed function, then the claim term is not a means-plus-function limitation.

21. I have been informed that a claim may be invalid under the patent laws of the United States if it is "indefinite." I have been informed that a claim is indefinite if, when viewed in light of the specification and prosecution history, it does not inform those skilled in the art of the scope of the invention with reasonable certainty.

22. I have also been informed that when a claim uses a term susceptible to subjective interpretations, to avoid indefiniteness, the patent must provide some objective standard in order to allow the public to determine the scope of the claimed invention.

IV. LEVEL OF ORDINARY SKILL IN THE ART

23. As noted, I understand that the level of ordinary skill in the art is assessed at the time of the patent's effective filing date. Because the '541 patent, the '598 patent, and the '422 patent each have different effective filing dates, I address the level of ordinary skill for each of these patents independently.

24. I have been told to assume for the purposes of this declaration that the effective filing date for the '541 patent is July 3, 2002, the date of filing of the provisional application to which the '541 patent claims priority on its face. In my opinion, a person of ordinary skill in the art as of July 2002 would be a computer systems engineer with a B.S. (or similar advanced degree) in electrical engineering, computer engineering, computer sciences, or a related field, and two or more years of experience in computer or network security. To the extent that I am provided with further information relevant to the effective filing date of the '541 patent, I reserve my right to amend my analysis accordingly.

25. I have been told to assume for the purposes of this declaration that the effective filing date for the '598 patent is also July 3, 2002, the date of filing of the provisional application to which the '598 patent claims priority on its face. Because the '598 patent and the '541 patent address similar technology and appear to share an effective filing date, in my opinion, a person of ordinary skill in the art for the '598 patent would have the same qualifications as the person of ordinary skill in the art for the '541 patent. To the extent that I am provided with further information relevant to the effective filing date of the '598 patent, I reserve my right to amend my analysis accordingly.

26. I have been told to assume for the purposes of this declaration that the effective filing date for the '422 patent is June 30, 2009, the date of filing of the provisional application to which the '422 patent claims priority on its face. Like, the '541 patent and the '598 patent, the '422 patent is similarly directed to computer security concepts. Accordingly, in my opinion, a person of ordinary skill in the art as of June 2009 would also be a computer systems engineer with a B.S. (or similar advanced degree) in electrical engineering, computer engineering, computer

sciences, or a related field, and two or more years of experience in computer or network security. To the extent that I am provided with further information relevant to the effective filing date of the '422 patent, I reserve my right to amend my analysis accordingly.

V. PERSON OF ORDINARY SKILL'S UNDERSTANDING OF THE CLAIMS

A. "an indication of an operation of the at least one operating system" ('422 patent, claims 1, 20)

27. I have been asked by counsel to review the phrase "an indication of an operation of the at least one operating system" of claims 1 and 20 of the '422 patent. Specifically, I have been asked to determine whether the claim phrase is definite—that is, whether the patent informs one of ordinary skill in the art of the scope of the invention with reasonable certainty.

28. Claim 1 uses this claim phrase as follows: "transmitting information to at least one collection computer about potential malicious activity when the operation of the at least one virtual browsing environment includes potential malicious activity, the information including at least one website address and an indication of an operation of the at least one operating system when the at least one browser application executed within the at least one virtual browsing environment accessed at least one website at the at least one website address."

29. The phrase, as set forth in claim 20, is presented in the same manner as claim 1.

30. The specification clearly teaches the skilled artisan what qualifies as "an indication of an operation of the at least one operating system." First, the specification explains that when a browser application in a virtual browsing environment accesses a website, a monitoring application ("VCMA") monitors operations in the virtual browsing environment. '422 patent at 13:1-7. As noted elsewhere, this would include monitoring of the operations of the operating system within the virtual browsing environment. '422 patent at 4:37-40. The specification also notes: "The information about each VBE's [virtual browsing environment's] operation may include the websites accessed by the browser application 304 and the browser applications interactions with the guest operating system 203." '422 patent at 13:7-10. The specification also provides examples of the types of information monitored, which include operations of the guest

operating system, such as attempts to execute applications or access memory. '422 patent at 13:11-20. The VCMA (monitoring application) then provides information indicating the identified operations to a control application ("VCA"), which may forward the information on to a collection computer. '422 patent at 13:4-7, 14:42-46.

31. Based on this disclosure, one of ordinary skill in the art would understand the scope of the claim phrase "an indication of an operation of the at least one operating system" with reasonable certainty to carry its plain meaning—information indicating actions performed by the operating system.

32. Because the patent informs one of ordinary skill in the art of the scope of the phrase "an indication of an operation of the at least one operating system," I conclude that this term is not indefinite.

B. "switching system for selectably and independently coupling and decoupling the processing logic device with the first storage and/or the second storage under automated control" ('541 patent, claims 1, 2, 8)

33. I have been asked by counsel to review the "switching system for selectably and independently coupling and decoupling the processing logic device with the first storage and/or the second storage under automated control" of claims 1, 2, and 8 of the '541 patent. Specifically, I have been asked to determine whether "switching," "system," or "switching system" imply or suggest structure—as opposed to functionality—to one of ordinary skill in the art.

34. One of ordinary skill at the time of the '541 patent was filed would not have understood "switching" to be a term of art. Instead, the skilled artisan would have understood it in its plain and ordinary way to refer to the function of changing from one element to another. "Switching" does not imply any reasonably certain structure and, indeed, one of ordinary skill in the art would understand that, in the context of the claim, switching could be done logically, meaning that it could merely refer to the function of a software operation on some hardware device. Accordingly, I conclude that the term "switching" does not connote physical structure to one of ordinary skill in the art.

35. Similarly, one of ordinary skill at the time of the '541 patent was filed would not have understood "system" to be a term of art. Instead, the skilled artisan would have understood it in its plain and ordinary way to refer to a means of organizing. For example, you could have a system for paying your bills in which you write a check, address an envelope, and affix a stamp. No structure would be implied simply because the methodology is called a system. Accordingly, I conclude that the term "system" does not connote physical structure to one of ordinary skill in the art.

36. Even when combined, "switching system" is not a term of art in computer networking. For the same reasons that "switching" does not imply any structure, a "switching system" suggests to the skilled artisan only an organized effort to perform the task of switching. Thus, for the same reasons addressed in the previous two paragraphs, I conclude that the phrase "switching system" does not imply or suggest structure to one of ordinary skill.

C. "website address" ('422 patent, claims 1, 20)

37. I have been asked by counsel to review the term "website address" of claims 1 and 20 of the '422 patent. Specifically, I have been asked to determine what a person of ordinary skill in the art would understand this term to mean.

38. The specification of the '422 patent explains that "the browser helper application 306 may record websites accessed by the browser application 304." '422 patent at 6:49-51. One of ordinary skill would understand that this "recorded website" would reflect a website address.

39. A person of ordinary skill in the art would certainly understand the term "website address" to refer to information used to identify a server hosting a website. One of ordinary skill would further understand that such information could take several forms, such as a Uniform Resource Locator (*e.g.*, www.* addresses commonly entered into a web browser, otherwise referred to as URL) or IP addresses. The skilled artisan would recognize that entry of either a URL or the IP address of a server hosting a website into a web browser search field would result in retrieval of the corresponding web page.

40. Nothing in the intrinsic record of the '422 patent alters this general understanding. To the contrary, the intrinsic record supports this understanding.

41. For example, the specification indicates that a URL could be used to identify a website's server, noting that "a user may specify a desired website in various ways, such as by typing a URL in an address line of the browser application 304." '422 patent at 10:58-61. Further, the provisional application to which the '422 patent claims priority, describes a methodology for providing a secure URL, utilizing an IP address as an identifier of the host website. Ex. J at 6. Similarly, the specification incorporates by reference a whitepaper entitled "Efficiently Tracking Application Interactions using Lightweight virtualization" by Yih Huang, et al. ("Huang"). '422 patent at 5:23-29. Huang also identifies an IP address as the website address for cnn.com. Ex. K at 3 ("we create a socket to connect to 64.236.16.20 on port 80 (one of the IP addresses of cnn.com).").

42. Accordingly, I conclude that one of ordinary skill in the art would understand "website address" to carry its plain and ordinary meaning, specifically information used to identify a server hosting a website.

D. "couple," "decouple," and variants ('541 patent, claims 1-2, 8, 11-12, and 16; '598 patent, claims 62 and 68)

43. I have also been asked to consider the terms "couple," "decouple," and their variations found in claims 1-2, 8, 11-12, and 16 of the '541 patent, and claims 62 and 66 of the '598 patent. The patents do not define these terms, but use them consistently with the meaning of these terms used in the art. In the electrical and computer engineering field, "coupled" and "decoupled" have broad meanings. For example, the standard dictionary prepared by the Institute of Electrical and Electronics Engineers ("IEEE") defines "coupled" or "coupling" as "[t]he association of two or more circuits or systems in such a way that power or signal information may be transferred from one to another." IEEE Standard Dictionary of Electrical and Electronics Terms at 229-31 (6th ed. 1996). Similarly, the definition of "decoupled" is "to separate (joined

or coupled subsystems) thereby enabling them to exist and operate separately." IEEE Standard Dictionary of Electrical and Electronics Terms at 412 (6th ed. 1996).

44. The '541 and '598 specifications use these terms consistently with those meanings. For example, the '541 patent specification explains that, with respect to Figure 2, "[t]he computing environments 1508 are or may be coupled or selectably coupleable to peripherals 1514-1, … , 1514-N via optional I/O Switch system 1510." '541 patent at 16:38-41. The patent identifies a similar example in a switch or switching system that includes "circuitry ... for coupling ... storage with logic circuitry such as with a CPU." *Id*. at 47:51-57. The patent notes that "coupling may involve any of a variety of switching schemes, such as ... altering one or more electrical connection[s]." *Id*. at 18:42-49. The '598 patent explains that a physical switch "opens or closes a predetermined electrical circuit" and may "turn on or off the power supply to a device to be switched." '598 patent at 7:16-20. Further, "[t]he data store switch system includes the functionality of a general switch system, where the source may represents [sic] a data store and the destination may represent a computing environment. The general configuration may be used to identify which data stores are coupled with which computing environments. *Id*. at 73:48-53. All of these examples indicate an association of at least two circuits or systems to transfer power or information from one to the other.

45. The patent specifications use the terms "decouple" and "decoupling" to indicate separating coupled devices. For example, switches and switching elements are used to "decouple the signals and data of interest between the storage 2321 and the logic means" and may include circuitry for "decoupling storage with logic circuitry such as with a CPU." '541 patent at 47:51-57. Figure 11 of the '541 patent emphasizes this point by illustrating circuit switches that allow the physical separation of the "storage" and "processor/CPU/ASIC" that both continue to exist and operate after separation.

46. Therefore, I conclude that one of ordinary skill in the art would understand "couple" and its variants, as used in the '541 and '598 patent claims, to carry the plain and ordinary meaning in the art: "[t]he association of two or more circuits or systems in such a way that power or signal

information may be transferred from one to another." Similarly, I conclude that one of ordinary skill in the art would understand "decouple" and its variants, as used in the '541 and '598 patent claims, to carry the plain and ordinary meaning in the art: "to separate (joined or coupled subsystems) thereby enabling them to exist and operate separately."

E. Unintelligible Claim Terms

47. Counsel has asked me to review two claim terms from the '541 patent and one from the '598 patent to determine whether one of ordinary skill in the art would be able to determine the scope of the invention with reasonable certainty.

48. First, I have been asked to consider the claim phrase "may not be coupled or only restrictively coupled to communicate" of claim 1 of the '541 patent. In context, the claim language reads: "the processing logic device may not be coupled or only restrictively coupled to communicate known information with the first storage when the processing logic is loaded with a program instruction that may be capable of executing a data item that has untrusted content or that did not originate within a known control environment."

49. This claim language is ambiguous because one of ordinary skill in the art could interpret it in more than one way. For example, the phrase could have been intended to be "may not be coupled[,] or [may be] only restrictively coupled[,] to communicate known information" or it could have been intended to be "may not be coupled[,] or [not be] only restrictively coupled[,] to communicate known information." Furthermore, due to the absence of punctuation, it would not be readily apparent to one of ordinary skill whether the "communication of known information" clause was intended to modify both the situation where the processing logic device may not be coupled **and** the situation where there is only restrictive coupling, or if it modifies only the latter situation. Accordingly, I conclude that this claim is indefinite because one of ordinary skill in the art could not discern its scope.

50. Second, I have been asked to consider the claim phrase "and automatically erased after each processing has occurred independent if the processing completed with error condition or without error condition" of claim 11 of the '541 patent. For context, claim 11 recites: "An

information appliance as in claim 8, wherein the second storage is configured to perform as a temporary storage during a processing operation when it is coupled with the processing logic device and automatically erased after each processing has occurred independent if the processing completed with error condition or without error condition, where an error condition may include detection of a virus or other malicious code execution."

51. The claim phrase is simply indecipherable. First, there seem to be words omitted after the phrase "each processing." It could have been intended to be "automatically erased after each processing [logic coupling] has occurred" or it could have been intended to be "automatically erased after each processing [operation] has occurred." But the addition of these words gives the claim two entirely different scopes.

52. Additionally, it is unclear what the word "independent" is intended to modify. It could apply to "processing [logic coupling]," "processing [operation]," "error condition," "temporary storage," or some other noun. Once again, the proper association would change the scope of the claim.

53. Also, there is a conditional "if" phrase without any corresponding result.

54. Considering each of these issues either individually or in combination, one of ordinary skill in the art would not be able to determine, with any reasonable certainty, the scope of the claim phrase "and automatically erased after each processing has occurred independent if the processing completed with error condition or without error condition." Accordingly, I conclude that the claim is indefinite.

55. Third, I have been asked to consider the claim phrase "if said correct health then said data store switch remains is not altered" in claim 62 of the '598 patent. For context, claim 62 recites: "if said corruption health is determined then said data store switch is operative to decouple said accessible data store and said selected processing environment, and communicatively couple a second accessible data store and said selected processing environment, if said correct health then said data store switch remains is not altered."

56. This language also provides languages that cannot be definitively resolved. For example, the clause "remains is not altered" is simply unintelligible. In addition, it appears that some condition was intended by the phrase "if said correct health," but the condition was not included in the claim language, rendering it impossible to determine if the condition is satisfied such that the corresponding result applies. Accordingly, one of ordinary skill in the art would be unable to determine, with reasonable certainty, the scope of the claim term "if said correct health then said data store switch remains is not altered." Therefore, I conclude that the claim is indefinite.

F. Subjective Claim Terms

57. I have been asked to review one claim term from the '541 patent and two terms from the '598 patent to determine whether the terms, in view of the specification, would enable one of ordinary skill in the art to determine their scope.

58. First, I have been asked to review the term "untrusted content" from claims 1 and 12 of the '541 patent. One of ordinary skill would recognize that the word untrusted is subjective and depends upon the standard one uses to determine whether content in trusted or untrusted. Claims 1 and 12 indicate what the system should do if there is untrusted content, but does not explain how to determine if the content is untrusted. For example, claim 1 recites: "the processing logic device may be coupled with the first storage when the processing logic is loaded with a program instruction not capable of executing a data item that has untrusted content or that did not originate within a known controlled environment." As noted, it is not possible to tell from the claim language when content is untrusted such that the program instruction is not capable of executing the data item in which the content is contained. Therefore, it is not possible for one of ordinary skill in the art to understand the scope of this term based on the claim language alone.

59. The specification provides no assistance, either. It uses the term "untrusted" or "untrusted content," or similar variations in the same way that the terms are used in the claim. That is, it provides no explanation of how one would determine that the content is untrusted. The specification does explain that "[i]f the file is unknown or untrusted it may be labeled for example 'untrusted', whereas if the file was created from within in a pristine environment, the

control environment may label the file as 'trusted'." '541 patent at 65:60-64. But that statement identifies "untrusted" data as "untrusted" providing a circular definition that precludes any objective understanding of the full scope of the term.

60. Because neither the claims nor the specification provide any objective standard from one of ordinary skill could to determine the scope of "untrusted data," I conclude that the term "untrusted data" is indefinite.

61. I have also been asked to consider the term "corruption health" of claim 62 of the '598 patent. On its face, one of ordinary would be unable to determine the scope of "corruption health" because it lacks any inherent standard for judging what degree of corruption is required to categorize a file as having "corruption health." The claim provides no assistance, indicating: "said instruction for analyzing said accessible data store to determine a health of said accessible data store; said health selected from a group of healths consisting of: a corruption health, and a correct health; if said corruption health is determined then said data store switch is operative to decouple said accessible data store and said selected processing environment, and communicatively couple a second accessible data store and said selected processing environment." Thus, with regard to corruption health, the claim teaches merely what occurs if there is "corruption health," but not how to determine when such a health status occurs.

62. The specification indicates that there are varying levels of corruption, noting that "[t]he corruption of hard drive 1 could be so terrible that the computer could not even 'boot up.'" '598 patent at 17:46-48. But it provides no guidance as to how much corruption is required to qualify the data store as having "corruption health." Thus, "corruption health" is subjective and fails to enable one of ordinary skill to determine the scope of term. Therefore, I conclude that it is indefinite.

63. I have also been asked to consider the term "correct health" of claim 62 of the '598 patent. "Correct health" arises in the same context as "corruption health" and has essentially the same problem. As with "corruption health," the claim only explains what happens if a data store has "correct health." However, it provides no explanation of how to determine when that status

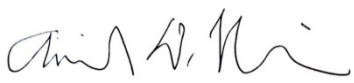
is achieved. The specification makes no mention of "correct health" other than repeating the language of the claims and thus fails to assist. One of ordinary skill in the art would certainly consider an unpopulated, completely clean data store as having "correct health," but the specification provides no explanation how far the data store can diverge from that state before it no longer is classified as having "correct health." Thus, "correct health" is subjective and fails to enable one of ordinary skill to determine the scope of term. Therefore, I conclude that it is indefinite.

* * *

64. The '598 patent specification indicates that Figure 2 is a schematic of a data-store switch. Figure 2 depicts various voltages, electrical grounding ports, resistors, connection ports, optical isolators ("optoiso"), an AD cable, and a 6 volt lithium battery. Those are components that are only present in physical devices—not software.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed: December 23, 2015



Aviel D. Rubin, Ph.D

APPENDIX A

Avi Rubin's Vita

Academic Degrees

- 1994, Ph.D., Computer Science and Engineering, University of Michigan, Ann Arbor
- 1991, M.S.E., Computer Science and Engineering, University of Michigan, Ann Arbor
- 1989, B.S., Computer Science (Honors), University of Michigan, Ann Arbor

Academic Appointments

- April, 2004 - present
  Professor, Johns Hopkins University

1. -August, 2010 - July, 2011
   Visiting Research Professor, Fulbright Scholar, Tel Aviv University, Israel

- January, 2003 - April, 2004
  Associate Professor, Johns Hopkins University

- January, 2003 - present
  Technical Director, Johns Hopkins University Information Security Institute

- 2006 - 2010
  Director and Principal Investigator (PI), National Science Foundation's ACCURATE Center

- 1995 - 1999
  Adjunct Professor, New York University

1. -*Internet and Web Security* Spring, 1999 (with Dave Kormann)

2. -*Privacy in Networks: Attacks and Defenses* Spring, 1998 (with Dave Kormann and Mike Reiter)
3. -*Design and Analysis of Cryptographic Protocols* Fall, 1996 & Spring, 1997 (with Matt Franklin)
4. -*Cryptography and Computer Security* Fall, 1995 & Spring, 1996

- Summer, 1999
Visiting Professor, École Normale Supérieure, Paris, France

- 1988 - 1993
Teaching Assistant, University of Michigan

1. -1993 *Intro. to Cryptography*
2. -1992 *Assembler Language Programming*
3. -1991 *Software Engineering*
4. -1990 *IVHS Seminar*
5. -1989-1990 **Head TA**, *Intro. to Computer Science*
6. -1988-1989 *Intro. to Computer Science*

- **Doctoral Committees**

1. -**Doctoral Thesis Advisor:** Gabe Kaptchuk, JHU
2. -**Doctoral Thesis Advisor:** Gary Truslow, JHU
3. -**Doctoral Thesis Advisor:** Paul Martin, JHU
4. -**Doctoral Thesis Advisor:** Michael Rushanan, JHU
5. -**Doctoral Thesis Advisor:** Ayo Akinyele, JHU (December, 2013)
6. -**Doctoral Thesis Advisor:** Matthew Pagano, JHU (August, 2013)
7. -**Doctoral Thesis Advisor:** Ryan Gardner, JHU (August, 2009)
8. -**Doctoral Thesis Advisor:** Sam Small, JHU (May, 2009)
9. -**Doctoral Thesis Advisor:** Sujata Doshi, JHU (May, 2009)
10. -**Doctoral Thesis Advisor:** Joshua Mason, JHU (June, 2009)
11. -**Dissertation Committee:** J. Alex Halderman, Princeton University (May, 2009)
12. -**Dissertation Committee:** Sophie Qiu (May, 2007).
13. -**Doctoral Thesis Advisor:** Adam Stubblefield (April, 2005).
14. -**Dissertation Committee:** Kevin FU, MIT (February, 2005).
15. -**Dissertation Committee:** Robert Fischer, Harvard University (June, 2003).
16. -**Dissertation Committee:** Marc Waldman, New York University, (April, 2003).
17. -**Dissertation Committee:** Patrick McDaniel, University of Michigan (September, 2001).
18. -**Doctoral Thesis Advisor:** Fabian Monrose, New York University (April, 1999).
19. -**Dissertation Committee:** Mike Just, Carleton University (November, 1998).
20. -**Dissertation Committee:** Trent Jaeger, University of Michigan (October, 1996).

Industry Experience

- 2011 - present
Harbor Labs, Managing Member
- 2005 - 2011
Independent Security Evaulators, Founder & President

- 1997 - 2002
  AT&T Labs - Research, Secure Systems Research Department
- 1994 - 1996
  Bellcore, Cryptography and Network Security Research Group
- Summer, 1990
  Great Lakes Software Co., *Programmer*, Howell, MI
- Summer, 1989
  IBM, *Programmer*, Meyers Corners Lab, Poughkeepsie, NY

Books

1. -Aviel D. Rubin, *Brave New Ballot*, Random House, (September, 2006).
2. -William R. Cheswick, Steven M. Bellovin and Aviel D. Rubin, *Firewalls and Internet Security: Repelling the Wily Hacker (2e)*, Addison Wesley Publishing Company, Inc., (February, 2003).
3. -**Chapter 4**, *Communications Policy and Information Technology: Promises, Problems, Prospects*, MIT Press, Lorrie Faith Cranor and Shane Mitchell Greenstein, eds., (2002).
4. -Aviel D. Rubin, *White-hat Security Arsenal*, Addison Wesley Publishing Company, Inc., (June, 2001).
5. -**Chapter 8**, *Publius* and **Chapter 14**, *Trust in Distributed Systems*, Marc Waldman, Lorrie Faith Cranor, and Aviel D. Rubin, *Peer-to-Peer*, O'Reilly & Associates, Inc., (February, 2001).
6. -Aviel D. Rubin, Daniel Geer, Marcus J. Ranum, *Web Security Sourcebook*, John Wiley & Sons, Inc , (June, 1997).
7. -**Ph.D. dissertation:** *Nonmonotonic Cryptographic Protocols* (ps.gz, pdf), University of Michigan, Ann Arbor (April, 1994).

Refereed Journal Publications

1. -David Kotz, Kevin Fu, Carl Gunter, Avi Rubin, *Security for Mobile and Cloud Frontiers in Healthcare,* Communications of the ACM (July, 2015).
2. -Ayo Akinyele, Christina Garman, Matthew D. Green, Ian Miers, Matthew Pagano, Aviel D. Rubin, Michael Rushanan, *Charm: A Framework for Rapidly Prototyping Cryptosystems,* Journal of Cryptographic Engineering (JCEN), (January, 2013).
3. -Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *Detecting Code Alteration by Creating a Temporary Memory Bottleneck*, IEEE Transactions on Information Forensics and Security: Special Issue on Electronic Voting, (December, 2009).
4. -Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, Avi Rubin, *Anonymity in Wireless Broadcast Networks*, International Journal of Network Security (IJNS), (January, 2008).
5. -Stephen Bono, Aviel Rubin, Adam Stubblefield, and Matthew Green, *Security Through Legality*, Communications of the ACM (June, 2006).
6. -Adam Stubblefield, Dan S. Wallach, and Aviel D. Rubin, *Managing the Performance Impact of Web Security*, Electronic Commerce Research Journal, February, 2005.
7. -David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, *Analyzing Internet Voting Security*, Communications of the ACM (October, 2004).

8. -Simon Byers, Aviel D. Rubin, and David Kormann, *Defending Against an Internet-based Attack on the Physical World*, ACM Transactions on Internet Technology (TOIT), August, 2004.
9. -Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *A Key Recovery Attack on the 802.11b Wired Equivalent Privacy Protocol (WEP)* (pdf), ACM Transactions on Information and System Security, May, 2004.
10. -Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, Communications of the ACM (December, 2002).
11. -Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *The Architecture of Robust Publishing Systems*, ACM Transactions on Internet Technology (TOIT), (November, 2001).
12. -David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single Signon Protocol,* Computer Networks, (July, 2000).
13. -Christian Gilmore, David P. Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, IEEE Network, (November, 1999).
14. -Fabian Monrose and Aviel D. Rubin, *Keystroke Dynamics as a Biometric for Authentication*, (pdf) Future Generation Computer Systems, (March, 2000).
15. -Michael K. Reiter and Aviel D. Rubin, *Anonymity Loves Company: Anonymous Web Transactions with Crowds* (ps.gz, pdf) Communications of the ACM (February, 1999).
16. -Aviel D. Rubin and Daniel E. Geer, Jr., *Mobile Code Security* (ps.gz, pdf), IEEE Internet Computing (November/December, 1998).
17. -Aviel D. Rubin and Daniel E. Geer, Jr., *A Survey of Web Security*, IEEE Computer, (September, 1998).
18. -Michael K. Reiter and Aviel D. Rubin, *Crowds: Anonymity for Web Transactions* (ps.gz, pdf), ACM Transactions on Information and System Security, (June, 1998).
19. -Aviel D. Rubin, *An Experience Teaching a Graduate Course in Cryptography* (ps, pdf), Cryptologia (April, 1997).
20. -Aviel D. Rubin, *Extending NCP for public Key Protocols*, Mobile Networks and Applications (ACM/Balzer), 2(3) (April, 1997).
21. -Aviel D. Rubin, *Independent One-Time Passwords*, (ps.gz, pdf) USENIX Journal of Computer Systems (February, 1996).
22. -Aviel D. Rubin, *Secure Distribution of Documents in a Hostile Environment*, Computer Communications (June, 1995).

Refereed Conference Publications

1. -Aviel D. Rubin, *Taking Two-Factor to the Next Level: Protecting Online Poker, Banking, Healthcare and Other Applications*, Proceedings of the 2014 Annual Computer Security Applications Conference, Invited Keynote Essay, (December, 2014).
2. -Michael Rushanan, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, *Security and Privacy in Implantable Medical Devices and Body Area Networks*, IEEE Symposium on Security and Privacy - SoK Track (May, 2014).
3. -Christina Garman, Matthew Green, Ian Miers, Aviel D. Rubin, *Rational Zero: Economic Security for Zerocoin with Everlasting Anonymity,* 1st Workshop on Bitcoin Research (March, 2014).
4. -Paul Martin, Avi Rubin and Rafae Bhatti, *Enforcing Minimum Necessary Access in Healthcare Through Integrated Audit and Access Control,* Health Informatics Symposium at the ACM Conference on Bioinformatics, Computational Biology, and Biomedical Informatics, (September, 2013).

5. -Ian M. Miers, Christina Garman, Matthew D. Green, Aviel D. Rubin, *Zerocoin: Anonymous Distributed e-Cash from Bitcoin*, Proc. IEEE Symposium on Security and Privacy (May, 2013).
6. -Ian M. Miers, Matthew D. Green, Christoph U. Lehmann, Aviel D. Rubin, *Vis-à-Vis Cryptography: Private and Trustworthy In-Person Certifications*, In Proceedings of the 3rd USENIX/HealthSec Workshop, (August, 2012).
7. -Joseph A. Akinyele, Matthew W. Pagano, Matthew D. Green, Christoph U. Lehmann, Zachary N. J. Peterson and Aviel D. Rubin, *Securing Electronic Medical Records Using Attribute-Based Encryption On Mobile Devices*, ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices, (October, 2011).
8. -Matthew D. Green, Aviel D. Rubin, *A Research Roadmap for Healthcare IT Security inspired by the PCAST Health Information Technology Report - 4 page Extended Abstract*, In Proceedings of the 2nd USENIX/HealthSec Workshop, (August, 2011).
9. -Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Designing for Audit: A Voting Machine with a Tiny TCB*, Financial Cryptography Conference, (January , 2010).
10. -Ryan Gardner, Sujata Garera, Matthew W. Pagano, Matthew D. Green, Aviel D. Rubin, *Securing Medical Records on Smart Phones, Workshop on Security and Privacy in Medical and Home-Care Systems*, (November, 2009).
11. -Ryan Gardner, Sujata Garera, Aviel D. Rubin, *Coercion Resistant End-to-end Voting*, Financial Cryptography Conference, (February, 2009).
12. -Ryan Gardner, Sujata Garera, Anand Rajan, Carols Rozas, Aviel D. Rubin, Manoj Sastry, *Protecting Patient Records from Unwarranted Access*, Future of Trust in Computing, (July, 2008).
13. -Sujata Garera, Niels Provos, Monica Chew and Aviel D. Rubin, *A Framework for Detection and Measurement of Phishing Attacks*, 5th ACM Workshop on Recurring Malcode (WORM 2007), (November, 2007).
14. -Sujata Garera and Aviel D. Rubin, *An Independent Audit Framework for Software Dependent Voting Systems*, 14th ACM Conference on Computer and Communications Security, (November, 2007).
15. -Ryan Gardner, Sujata Garera, and Aviel D. Rubin, *On the Difficulty of Validating Voting Machine Software with Software*, In Proceedings of the 2nd USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '07), (August, 2007).
16. -Sujata Doshi, Fabian Monrose, and Aviel D. Rubin, *Efficient Memory Bound Puzzles using Pattern Databases*, 4th International Conference on Applied Cryptography and Network Security (ACNS'06), (June, 2006).
17. -Sophie Qiu, Patrick McDaniel, Fabian Monrose, and Avi Rubin, *Characterizing Address Use Structure and Stability of Origin Advertisement in Interdomain Routing*, 11th IEEE Symposium on Computers and Communications, (June 2006).
18. -Zachary Peterson, Randal Burns, Joseph Herring, Adam Stubblefield, and Aviel D. Rubin, *Secure Deletion for a Versioning Filesystem* , Proc. USENIX Conference on File and Storage Technologies (FAST '05), (December, 2005).
19. -Stephen C. Bono, Matthew Green, Adam Stubblefield, Ari Juels, Aviel D. Rubin, Michael Szydlo, *Security Analysis of a Cryptographically-Enabled RFID Device* 14th USENIX Security Symposium, (August, 2005).

20. -Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System*, Proc. IEEE Symposium on Security and Privacy (May, 2004).
21. -Nathanael Paul, David Evans, Aviel D. Rubin and Dan Wallach, *Authentication for Remote Voting*, ACM Workshop on Human-Computer Interaction and Security Systems (April, 2003).
22. -Matt Blaze, John Ioannidis, Angelos D. Keromytis, Tal Malkin, and Aviel Rubin, *Protocols for Anonymity in Wireless Networks,* Proc. 11th International Workshop on Security Protocols (April, 2003).
23. -Geoffrey Goodell, William Aiello, Timothy Griffin, John Ioannidis, Patrick McDaniel, Aviel Rubin, *Working Around BGP: An Incremental Approach to Improving Security and Accuracy of Interdomain Routing* , Proc. ISOC Symposium on Network and Distributed System Security (February, 2003).
24. -Simon Byers, Aviel D. Rubin, David Kormann, *Defending Against an Internet-based Attack on the Physical World* (pdf), ACM Workshop on Privacy in the Electronic Society (November, 2002).
25. -Adam Stubblefield, John Ioannidis, and Aviel D. Rubin, *Using the Fluhrer, Mantin, and Shamir Attack to Break WEP*, Proc. ISOC Symposium on Network and Distributed System Security (February, 2002).
26. -Aviel D. Rubin, *Security Considerations for Remote Electronic Voting*, 29th Research Conference on Communication, Information and Internet Policy (TPRC2001), (October, 2001).
27. -Aviel D. Rubin and Rebecca N. Wright, *Off-line generation of limited-use credit card numbers*, (ps.gz, pdf) Financial Cryptography Conference, (February, 2001).
28. -Marc Waldman, Aviel D. Rubin, and Lorrie F. Cranor, *Publius, A robust, tamper-evident and censorship-resistant web publishing system*, 9th USENIX Security Symposium, (August, 2000).
29. -David P. Kormann and Aviel D. Rubin, *Risks of the Passport Single Signon Protocol*, 9th International World Wide Web Conference, (May, 2000).
30. -Patrick McDaniel and Aviel D. Rubin, *A Response to "Can we Eliminate Certificate Revocation Lists?"*, (ps.gz, pdf), Financial Cryptography Conference, (February, 2000).
31. -William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, *Using smartcards to secure a personalized gambling device* (ps.gz, pdf), 6th ACM Conference on Computer and Communications Security, (November, 1999).
32. -Ian Jermyn, Alain Mayer, Fabian Monrose, Michael K. Reiter, and Aviel D. Rubin, *The Design and Analysis of Graphical Passwords* (ps.gz, pdf) 8th USENIX Security Symposium, (August, 1999).
33. -Christian Gilmore, David Kormann, and Aviel D. Rubin, *Secure Remote Access to an Internal Web Server*, (ps.gz, pdf), Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).
34. -Fabian Monrose, Peter Wykoff, and Aviel D. Rubin, *Distributed Execution with Remote Audit* (ps.gz, pdf), Proc. ISOC Symposium on Network and Distributed System Security (February, 1999).

35. -Dahlia Malkhi, Michael K. Reiter and Aviel D. Rubin, *Secure Execution of Java Applets using a Remote Playground* (ps, pdf) Proc. IEEE Symposium on Security and Privacy (May, 1998).
36. -Aviel D. Rubin, Dan Boneh, and Kevin Fu, *Revocation of Unread E-mail in an Untrusted Network* (ps.gz, pdf), Second Australasian Conference on Information Security and Privacy (July, 1997).
37. -Fabian Monrose and Aviel D. Rubin, *Authentication via Keystroke Dynamics* (ps, pdf), 4th ACM Conference on Computer and Communications Security (April, 1997).
38. -David M. Martin, Siviramakrishnan Rajagopalan, and Aviel D. Rubin, *Blocking Java Applets at the Firewall* (ps, pdf), Proc. ISOC Symposium on Network and Distributed System Security (February, 1997).
39. -Trent Jaeger, Aviel D. Rubin and Atul Prakash, *A System Architecture for Flexible Control of Downloaded Executable Content*, 5th International Workshop on Object-Orientation in Operating Systems (October, 1996).
40. -Trent Jaeger, Aviel D. Rubin and Atul Prakash, *Building Systems that Flexibly Control Downloaded Executable Content*, Proc. 6th USENIX Security Symposium (July, 1996).
41. -Victor Shoup and Aviel D. Rubin, *Session Key Distribution Using Smart Cards*, (ps, pdf), Proc. of Eurocrypt '96 (May, 1996).
42. -Trent Jaeger & Aviel D. Rubin, *Preserving Integrity in Remote File Location and Retrieval*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1996).
43. -Aviel D. Rubin, *Extending NCP for Public Key Protocols*, Proc. IEEE 4th International Conference on Computer Communications and Networks (September, 1995).
44. -Aviel D. Rubin, *Pseudo-Random Functions for One-Time Passwords*, Proc. 5th USENIX UNIX Security Symposium (June, 1995).
45. -Aviel D. Rubin, *Trusted Distribution of Software Over the Internet*, Proc. ISOC Symposium on Network and Distributed System Security (February, 1995).
46. -Aviel D. Rubin & Peter Honeyman, *Nonmonotonic Cryptographic Protocols*, Proc. IEEE Computer Security Foundations Workshop VII (June, 1994).
47. -Aviel D. Rubin & Peter Honeyman, *Long Running Jobs in an Authenticated Environment*, Proc. 4th USENIX UNIX Security Symposium (October, 1993).

Patents

1. -Aviel D. Rubin, Utilization of multiple devices to secure online transactions, **US Patent Number 9,064,376**, (June 23, 2015).
2. -Steven M. Bellovin, Thomas J. Killian, Bruce LaRose, Aviel D. Rubin, Norman L. Schryer, Method and apparatus for connection to virtual private networks for secure transactions, **US Patent Number 8,239,531**, (August 7, 2012) and **8,676,916** (March 18, 2014).
3. -Christian A. Gilmore, David P. Kormann, and Aviel D. Rubin, Method and apparatus for secure remote access to an internal web server, **US Patent Number 7,334,126**, (February 19, 2008).
4. -Aviel D. Rubin, "Method for secure remote backup", **US Patent Number 7,222,233**, (May 22, 2007).

5. -Frederick Douglis, Michael Rabinovich, Aviel D. Rubin, and Oliver Spatscheck, "Method for content distribution in a network supporting a security protocol", **US Patent Number 7,149,803**, (December 12, 2006).
6. -William A. Aiello, Steven M. Bellovin, Charles Robert Kalmanek, Jr., William T Marshal, and Aviel D. Rubin, "Method and apparatus for enhanced security in a broadband telephony network", **US Patent Number 7,035,410**, (April 25, 2006).
7. -Aviel D. Rubin, "Broadband Certified Mail", **US Patent Number 6,990,581**, (January 24, 2006).
8. -William A. Aiello, Aviel D. Rubin, and Martin J. Strauss, "Using smartcards to enable probabilistic transaction on an untrusted device", **US Patent Number 6,496,808**, (December 17, 2002).
9. -Aviel D. Rubin and Victor J. Shoup, "Session Key Distribution Using Smart Cards", **US Patent Number 5,809,140**, (September 15, 1998).
10. -Aviel D. Rubin, "Method for the Secure Distribution of Electronic Files in a Distributed Environment", **US Patent Number 5,638,446**, (June 10, 1997).

Professional Activities

1. -Board of Directors

2. -Director, Maryland Israel Development Center (MIDC), (2013 - present).
3. -Director, USENIX Organization, elected by popular vote (2000 - 2004).

4. -Editorial and Committees

5. -**Associate Editor:** IEEE Transactions on Information Forensics and Security (2009-2011).
6. -**Associate Editor**: Communications of the ACM (CACM), 2009 - present.
7. -**Guest Co-Editor:** IEEE Transactions on Information Forensics and Security: *Special Issue on Electronic Voting*, December 1, 2009.
8. -**Guest Co-Editor:** IEEE Security & Privacy Magazine, *Special Issue on Electronic Voting*, October/November, 2007.
9. -**Associate Editor:** IEEE Transactions on Software Engineering (2005-2006).
10. -**Editorial and Advisory Board:** International Journal of Information and Computer Security (IJICS) (2004-2006).
11. -**Guest Co-Editor:** IEEE Computer Networks, *Special Issue on Web Security*, January, 2005.
12. -**Editorial Board:** Journal of Privacy Technology (2004-2006).
13. -**Guest Co-Editor:** IEEE Security & Privacy Magazine, *Special Issue on Electronic Voting Security*, January/February, 2004.
14. -**Member:** Security Peer Review Group (SPRG) of the Federal Voting Assistance Program's (FVAP) Secure Electronic Registration and Voting Experiment (SERVE) Project, 2003-2004.
15. -**Member:** DARPA Information Science And Technology Study Group (2003-2006).
16. -**Associate Editor:** IEEE Security & Privacy Magazine (2003-present).
17. -**Guest Editor:** Communications of the ACM, *Special Issue on Wireless Networking Security*, May, 2003.
18. -**Associate Editor:** ACM Transactions on Internet Technology (2002-2005).
19. -**Executive Committee Member:** DIMACS Workshop Series with Special Focus on Network Security (2002-2004).

20. -**Advisory Board Member:** Information Security and Cryptography Book Series, Springer, 2001-2006.
21. -**Member:** Steering Group, ISOC Symposium on Network and Distributed System Security, 2001-2004.
22. -**Member:** Government Infosec Science and Technology Study Group on malicious code, 1999 - 2000.
23. -**Member:** *AT&T Internet Intellectual Property Review Team*, 1999 - 2001.
24. -**Associate Editor:** *Electronic Commerce Research Journal*, Baltzer Science Publishers, 1999 - 2002.
25. -**Co-Editor:** Electronic Newsletter of the IEEE Technical Committee on Security & Privacy, with Paul Syverson, 1998.
26. -**Editorial Board:** Bellcore Security Update Newsletter, 1995-1996.

1. -Conference Committees

2. -Program Committee member: Financial Cryptography '15 Barbados, February, 2015.
3. -Program Committee member: USENIX HealthTech Workshop on Health Information Technologies (HealthTech ’15), August 11, 2015.
4. -Program Co-chair: (w/Eugene Vasserman) USENIX HealthTech Workshop on Health Information Technologies (HealthTech ’14), August 19, 2014.
5. -Program Committee member: 2nd USENIX Workshop on Health Security and Privacy (HealthSec '11), August 9, 2011.
6. -**Program Co-chair:** (w/Kevin Fu & Yoshi Kohno), 1st USENIX Workshop on Health Security and Privacy (HealthSec '10), August 10, 2010.
7. -Program Committee member: First Security and Privacy in Medical and Home-Care Systems Workshop (SPIMACS), Chicago, IL, November 13, 2009.
8. -Invited Talks Co-Coordinator: 17th USENIX Security Symposium, San Jose, CA, July 28 - August 1, 2008.
9. -**Program Co-chair:** (w/Patrick McDaniel): IEEE Symposium on Security and Privacy, Oakland, California, May 18-22, 2008.
10. -**Program Co-chair:** (w/Giovani Di Crescenzo): Financial Cryptography '06 Anguilla BWI, February, 2006.
11. -Program Committee member: IEEE Symposium on Security and Privacy, Oakland, California, May 9-12, 2004.
12. -Program Committee member: Financial Cryptography '04 Key West, Florida, February 9-12, 2004.
13. -Program Committee member: 2nd ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., October 30, 2003.
14. -Program Committee member: 10th ACM Conference on Computer and Communications Security, Washington D.C., October 27-30, 2003.
15. -Program Committee member: 8th European Symposium on Research in Computer Science (ESORICS), Norway, October 13-15, 2002.
16. -**Program Vice Chair:** Security and Privacy Track, The Twelfth International World Wide Web Conference, Budapest, Hungary, May 20-24, 2003.
17. -Program Committee member: IEEE Symposium on Security and Privacy, Oakland, California, May 11-14, 2003.
18. -Program Committee member: Workshop on Security and Assurance in Ad hoc Networks, Orlando, FL, January 28, 2003.

19. -Program Committee member: 4th International Conference on Information and Communications Security (ICICS), Kent Ridge Digital Labs (KRDL), Singapore December 9-12, 2002.
20. -Program Committee member: ACM SIGSAC Workshop on Privacy in the Electronic Society Washington D.C., November 21, 2002.
21. -Program Committee member: 9th ACM Conference on Computer and Communications Security, Washington D.C., November 17-21, 2002.
22. -Program Committee member: 5th International Conference on Electronic Commerce Research (ICECR-5), Montreal, Canada, October 23-27, 2002.
23. -Program Committee member: 2nd Symposium on Requirements Engineering for Information Security (SREIS), Raleigh, North Carolina, Oct 14-15, 2002.
24. -Program Committee member: 7th European Symposium on Research in Computer Science (ESORICS), Zurich, Switzerland, October 14-16, 2002.
25. -Program Committee member: 11th USENIX Security Symposium, San Francisco, Ca, August 5-9, 2002.
26. -Program Committee member: International Workshop on Global and Peer-to-Peer Computing at IEEE International Symposium on Cluster Computing and the Grid (CCGrid'2002), Berlin, Germany, May 21-24, 2002.
27. -Program Committee member: 11th International World Wide Web Conference Honolulu, Hawaii, May 7-11, 2002.
28. -Program Committee member: 2nd Workshop on Privacy Enhancing Technologies San Francisco, CA, April 14-15, 2002.
29. -Program Committee member: The 1st International Workshop on Peer-to-Peer Systems (IPTPS'02) MIT Faculty Club, Cambridge, MA, March 7-8, 2002.
30. -Program Committee member: The 4th International Conference on Telecommunications and Electronic Commerce Dallas, TX, November, 2001.
31. -Program Committee member: 10th USENIX Security Symposium, Washington D.C., August 13-17, 2001.
32. -Program Committee member: Financial Cryptography '01 Grand Cayman, Cayman Islands, BWI, February, 2001.
33. -**Program Co-chair:** (w/Paul Van Oorschot): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 7-9, 2001.
34. -Program Committee member: The 3rd International Conference on Telecommunications and Electronic Commerce Dallas, TX, November 16-19, 2000.
35. -Program Committee member: 9th USENIX Security Symposium, Denver, Colorado, August 14-17, 2000.
36. -Program Committee member: Workshop on Design Issues in Anonymity and Unobservability Berkeley, California, July 25-26, 2000.
37. -Program Committee member: Performance and Architecture of Web Servers (PAWS), Santa Clara, CA, June 18, 2000.
38. -**Program Co-chair:** (w/Gene Tsudik): ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 2-4, 2000.
39. -Program Committee member: 1999 International Information Security Workshop (ISW'99), Kuala Lumpur, Malaysia, November 6-7, 1999.
40. -Program Committee member: 2nd Int'l. Conference on Telecommunications and Electronic Commerce, Nashville, TN, October 6-8, 1999.
41. -Invited Talks coordinator: 8th USENIX Security Symposium, Washington D.C., August, 1999.

42. -**Program Chair:** 24th USENIX Annual Technical Conference, Monterey, CA, June 7-11, 1999.
43. -Program Committee member: 8th International World Wide Web Conference , Toronto, Canada, May 11-14, 1999.
44. -Program Committee member: 3rd USENIX workshop on Electronic Commerce , Boston, MA, August 31 - September 3, 1998.
45. -Program Committee member: 5th ACM Conference on Computer and Communications Security, San Francisco, CA, November 3-5, 1998.
46. -**Program Chair:** 7th USENIX Security Symposium, San Antonio, TX, Jan. 26-29, 1998.
47. -Program Committee member: 4th ACM Conference on Computer and Communications Security, Zurich, Switzerland, April 2-4, 1997.
48. -Program Committee member: 6th USENIX Security Symposium, San Jose, CA, July 22-25, 1996.
49. -Program Committee member: ISOC Symposium on Network and Distributed System Security, San Diego, CA, February 22-23, 1996.

1. -Panels

2. -**Panelist:** RSA Conference, Social Networks Security Panel, San Francisco, CA (April 21, 2015).
3. -**Panelist:** Expert Witness in Mock Trial: FTC Data Security, 63rd American Bar Association Section of Antitrust Law Spring Meeting Washington DC, (April 15, 2015).
4. -**Panelist:** Security in Electronic Medical Records Databases, Medicine 2.0 Workshop, Haifa, Israel, (April 7, 2011).
5. -**Panelist:** Security in the Cloud, Workshop on Cloud Security, Israeli Defense Ministry, Tel Aviv, Israel, (February 15, 2011).
6. -**Panelist:** Securing Information Technology in Healthcare (SITH), Security and Usability of Electronic Health Records, Dartmouth College, NH, (May 17, 2010).
7. -**Panelist:** First Security and Privacy in Medical and Home-Care Systems Workshop (SPIMACS), Authentication in iHealthcare, Chicago, IL, (November 13, 2009).
8. -**Panelist:** Computers, Freedom, and Privacy Conference, Internet Voting for Overseas Americans, Washington DC, (June 4, 2009).
9. -**Panelist:** Workshop on Electronic Voting, Electronic Voting: Future Aspirations, Tel Aviv, Israel (May 18, 2009).
10. -**Panelist:** RSA Conference, Exploiting Online Games, San Francisco, CA (April 23, 2009).
11. -**Panelist:** American Association for the Advancement of Science, *Revisiting the U.S. Voting System: A Research Inventory, Technology, Usability, and Security panel*, Washington DC, (November 27, 2006).
12. -**Panelist:** California Secretary of State's Voting System Testing Summit, *Security Panel*, Sacramento, CA, (November 28-29, 2005).
13. -**Panelist:** NIST Symposium on Voting System Threats, *Configuration and Usability Threats*, Gaithersburg, MD, (October 7, 2005).
14. -**Panelist:** Conference of State Supreme Court Chief Justices, *Voting Technologies*, Charleston, SC (August 1, 2005).
15. -**Panelist:** *Workshop on observation of automated elections*, The Carter Center, Atlanta, GA (March 18, 2005).
16. -**Panelist:** The Carter Center Venezuela Virtual Panel, (November, 2004).

17. -**Panelist:** Workshop on Voting, *Vote Capture and Vote Counting*, Harvard Kennedy School of Government, The Technologies of Voting, Cambridge, MA (June 1, 2004).
18. -**Panelist:** Computer Science and Telecommunications Board of The National Academy of Science *Workshop on Dependable Software Systems*, Case Study: Electronic Voting Washington D.C. (April 20, 2004).
19. -**Panelist:** USENIX Security 2003, *Electronic Voting*, Washington D.C. (August 6, 2003).
20. -**Panelist:** Democracy Now, 2003, *Voter-Verifiable Elections: How Do We Get There?*, Washington D.C. (November 23, 2003).
21. -**Panelist:** USENIX Security 2003, *Electronic Voting*, Washington D.C. (August 6, 2003).
22. -**Panelist:** IEEE Infocom 2002, *Securing Wireless and Mobile Networks - Is It Possible?*, New York City (June 25, 2002).
23. -**Participant:** 2002 Security Visionary Roundtable: *A Roadmap for a Safer Wireless World*, Washington D.C., (May 5-7,2002).
24. -**Panelist:** Computers Freedom and Privacy 2002, *Who Goes There? Privacy in Identity and Location Services*, San Francisco (April 18, 2002).
25. -**Panel moderator:** Conference on Democracy and the Internet in an Enlarging Europe *Overview of On-Line Voting: Systems and Issues*, New York, NY (March, 2001).
26. -**Panelist:** Financial Cryptography 2001, *The Business of Electronic Voting*, Grand Cayman (February, 2001).
27. -**Panelist:** National Science Foundation *E-voting workshop*, Washington, D.C., (October, 2000).
28. -**Panelist:** 5th ACM Conference on Computer and Communications Security, Anonymity on the Internet, San Francisco, CA, (November 1998).
29. -**Panelist:** Open Systems Security and ISSA Annual Conference, *Securing the Web*, Orlando, FL (March, 1998).
30. -**Panel organizer and moderator:** *Implementation Issues for Electronic Commerce: What Every Developer Should Know*. ISOC Symposium on Network and Distributed System Security, (March, 1998).
31. -**Panel organizer and moderator:** *Downloadable Executable Content - Past, Present and Future*. ISOC Symposium on Network and Distributed System Security (February, 1997).
32. -**Panelist:** DIMACS Workshop on Network Threats, Web/Java Security Issues, New Brunswick, NJ (December 5, 1996).

1. -Tutorials Taught

2. -The Mathematics of Information Technology and Complex Systems Network (MITACS), *Network Security*, (May 8, 2003).
3. -IEEE Infocom 2002, *End to End Web Security and E-commerce*, (June 23, 2002).
4. -2002 USENIX Annual Technical Conference, *Introduction to Computer Security*, (June 10, 2002).
5. -LISA 2001, 15th Systems Administration Conference, *Introduction to Computer Security*, (December, 2001).
6. -8th & 9th USENIX Security Symposia, *Cryptography - From the Basics Through PKI in 23,400 Seconds*, (August, 2000) & (August 1999), with Dan Geer.
7. -9th International World Wide Web Conference, *Security on the World Wide Web*, (May, 2000).

8. -ISOC Symposium on Network and Distributed System Security, *Cryptography 101*, (February, 2000).
9.

Testimony

Before Government Bodies

1. -United States Pentagon, High Level Security Briefing on the Security of Embedded Devices (January 15, 2014).
2. -United Stated House Committee on Science, Space, and Technology, *Full Committee Hearing - Is My Data on Healthcare.gov Secure?*, Washington, D.C., (November 19, 2013).
3. -United Stated House Committee on Oversight and Government Reform, *hearing on electronic voting*, Washington, D.C., (April 18, 2007).
4. -United Stated House Committee on Appropriations, *hearing on ensuring the integrity of elections*, Washington, D.C., (March 7, 2007).
5. -Maryland Senate Committee on Education, Health, and Environmental Affairs, Expert Testimony, *Hearing on Senate Bill 392 for Voter-Verified Records in Voting Systems*, Annapolis, MD, (February 22, 2007).
6. -Maryland House Ways and Means Committee, Expert Testimony, *Hearing on House Bill 18 for improving voting systems in Maryland*, Annapolis, MD, (February 1, 2007).
7. -Maryland House Ways and Means Committee, Expert Testimony, *Hearing on House Bill 244 requiring a voter verified paper record for voting machines in Maryland*, Annapolis, MD, (February 1, 2006).
8. -United States Election Assistance Commission, *Hearing on Voluntary Voting Systems Guidelines*, Expert Testimony, Panel on Voter Verified Paper Audit Trail, Washington D.C. (June 30, 2005).
9. -Senate hearing: *Voting in 2004: A Report to the Nation on America's Election Process*, Expert Testimony, Absentee Ballot Panel, Dirksen Senate Office Building, Washington, DC (December 7, 2004).
10. -United States Election Assistance Commission, Technical Guidelines Development Committee, Technology Panel, Expert Testimony, *Public Hearings on Computer Security and Transparency*, National Institute of Standards and Technology, Gaithersburg, MD, (September 20, 2004).
11. -United States House Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Expert Testimony, *Hearing on Electronic Voting*, Washington, D.C. (July 20, 2004).
12. -United States House Committee on House Administration, Expert Testimony, *Hearing on Security of Electronic Voting*, Washington, D.C. (July 7, 2004).
13. -United States Federal Trade Commission, Written Expert Testimony, on a proposed Do Not Email Repository, (May 10, 2004).
14. -United States Election Assistance Commission, Expert Testimony, *Hearing on Electronic Voting Security*, Technology Panel, Washington D.C. (May 5, 2004).

As an Expert in Litigation

1. -TVIIM. v. **McAfee Inc.**, Case # 3:13-cv-04545-VC, United States District Court, District of N. California. (*Patent Non-Infringement and Invalidity)*
2. -Expert Testimony at trial, San Francisco, CA (July, 2015).

3. -Expert Testimony at deposition, Baltimore, MD (February, 2015).
4. -Intellectual Ventures vs. **Symantec**, Case # 1:10-cv-01067-LPS, United States District Court, District of Delaware. (*Patent Invalidity)*
5. -Expert Testimony at trial, Wilmington, DE (February, 2015).
6. -Expert Testimony at deposition, Baltimore, MD (May, 2013).
7. **-Rovi Solutions & Veracode** vs. Appthority, Case # 12-10487-DPW, United States District Court, District of Massachusetts. (*Patent Infringement and Validity)*
8. -Expert Testimony at trial, Boston, MA (August 11, 2014).
9. -Expert Testimony at deposition, Baltimore, MD (April 4, 2014).
10. -**Juniper** vs. Palo Alto Networks, Case # 1:11-CV-01258-SLR, United States District Court, District of Delaware. (*Patent Infringement*)
11. -Expert Testimony at trial, Wilmington, DE (February, 2014).
12. -Expert Testimony in court hearing, Wilmington, DE (November 14, 2013).
13. -Expert Testimony at deposition, Baltimore, MD (June, 2013).
14. -Prism Technologies. v. **Adobe Systems Inc**., Case # 8:10-cv-00220-LES-TDT, United States District Court, District of Nebraska. (*Patent Invalidity)*
15. -Expert Testimony at deposition, Baltimore, MD (August, 2012).
16. -Finjan Inc. vs. **McAfee, Inc**., Case # 10-593 (GSM), United States District Court, District of Delaware. (*Patent Non-Infringement)*
17. -Expert Testimony at deposition, Washington, DC (June, 2012).
18. -Avaya Inc. vs. **Telecom Labs Inc,. TeamTLI.com Corp., and Continuant Technologies**, Case # 3:06-cv-02490 (GEB), United States District Court, District of New Jersey. (*Contract Dispute)*
19. - Expert Testimony at deposition, Newark, NJ (August, 2011).
20. -**Lear Automotive** vs. Johnson Controls Inc (JCI), Case # 04-CV-73461, United States District Court, Eastern District of Michigan. (*Patent Infringement and Validity)*
21. - Expert Testimony at trial, Detroit, MI (February, 2011).
22. - Expert Testimony at deposition, Baltimore, MD (December, 2005).
23. -**TecSec Inc** vs. International Business Machines Corporation, Case # 1:10-CV 115 LMB/TCB, United States District Court, Eastern District of Virginia. (*Patent Infringement)*
24. -Expert Testimony at deposition, Newark, NJ (November, 2010).
25. -**Echostar Satellite Corporation** vs. NDS Group, Case # SA CV 03-950 DOC(JTL), United States District Court, Central District of California. (*Copyright and DMCA)*
26. -Expert Testimony at trial, Santa Ana, CA (April, 2008).
27. -Expert Testimony at deposition, Santa Ana, CA (April, 2008).
28. -Expert Testimony at deposition, Baltimore, MD (October, 2007).
29. -**Web.com Inc** vs. The Go Daddy Group Inc., Case # CV07-01552-PHX-MHM, United States District Court, Arizona. (*Patent Infringement*)
30. -Expert Testimony at Markman hearing, Phoenix, Az (July, 2008).
31. -Expert Testimony at deposition, Baltimore, MD (May, 2008).
32. -z4 Technologies vs. **Microsoft & Autodesk**, Case # 2:04-CV-00335-LED, United States District Court, Eastern District of Texas. (*Patent Non-Infringement and Invalidity)*
33. -Expert Testimony at trial, Tyler, TX, (April, 2006).
34. -Expert Testimony at deposition, Washington DC (January, 2006).
35. -**Linda Schade** vs. Linda Lamone et. al., *Trial on the Legality of Paperless Voting Machines in Maryland*. (*Adequacy of Voting Equipment)*
36. -Expert Testimony at trial, Annapolis, MD (August 25, 2004).

Awards

1. -**Fulbright Scholar** in Israel at Tel Aviv University, academic year 2010-2011.
2. -2009, **Google Research Award**, *Securing Medical Records on Smartphones.*
3. -Chosen as one of **54 favorite people, places and things in Jewish Baltimore**, Baltimore Jewish Times, February 22, 2008.
4. -2007 Award for Outstanding Research in Privacy Enhancing Technologies, for *Security Analysis of a Cryptographically-Enabled RFID Device* (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
5. -2005 **Best Student Paper Award** at the 14th USENIX Security Symposium, *Security Analysis of a Cryptographically-Enabled RFID Device* (with Stephen C. Bono, Matthew Green, Ari Juels, Adam Stubblefield, Michael Szydlo).
6. -2004 **Electronic Frontiers Foundation** *Pioneer Award*.
7. -**Baltimorean of the Year**, Baltimore Magazine, January, 2004.
8. -2001 **Index on Censorship** *Freedom of Expression Award* for the Best Circumvention of Censorship for the Publius project.
9. -2000 **Best Paper Award** at the 9th USENIX Security Symposium, *A robust, tamper-evident and censorship-resistant web publishing system* (with Marc Waldman and Lorrie Cranor).
10. -1999 **Best Paper Award & Best Student Paper Award** at the 8th USENIX Security Symposium, *The Design and Analysis of Graphical Passwords* (with Ian Jermyn, Alain Mayer, Fabian Monrose, and Michael K. Reiter).
11. -1996 Co-author of **Best Student Paper**, *Building Systems that Flexibly Control Downloaded Executable Content*, at the 6th USENIX UNIX Security Symposium. Student: Trent Jaeger.
12. -1992 National Science Foundation Fellowship - Summer Institute in Japan
13. -1986 Branstrom Prize, University of Michigan

Technical Advisory Boards

Current Positions

1. -Fast Orientation
2. -Reason and respond to enterprise events

3. -ZeroFox
4. -Provide security for social networking

Past Successful Technical Advisory Board Positions

1. -Arbor Networks
2. -Acquired by Danaher, August, 2010.
3. -Authentica
   - Acquired by EMC Corporation, March, 2006.
1. -Fortify Software
2. -Acquired by Hewlett Packard, September 2010.

3. -Gilian Technologies
   - Acquired by Breach Security, Inc, July, 2004.
1. -Hx Technologies
   - Acquired by MEDecision, May, 2009.
1. -Indigo Security
   - Acquired by Tablus, February, 2005.
1. -NeoPath Networks
   - Acquired by Cisco, April, 2007.
1. -Netscaler
2. -Acquired Citrix Systems, August, 2005.
3. -SiteAdvisor
   - Acquired by McAfee, April, 2006.
1. -Tablus
2. -Acquired by EMC Corporation, August, 2007.